What is claimed is:

1. A system for analyzing and managing spam e-mail, comprising:

a database for storing rules for determining whether e-mail messages are spam;

a message processor that processes e-mail messages to determine whether any rules within the database are matched by the messages and to attach data to the messages regarding the rules that are matched; and

a spam analyzer that analyzes the data to determine attributes regarding the rules, and to dynamically modify rules within the database based on the data.

2. The system of claim 1 wherein the database stores the rules in one or more tables.

3. The system of claim 1 wherein the attributes comprise statistics.

4. The system of claim 3 wherein the statistics comprise at least one of the following: last updated, last hit, total hits, spam hits, nonspam hits, and false positive hits.

5. The system of claim 1 wherein each rule in the database is assigned an identification number and a score that is used to determine whether an e-mail message is spam.

6. The system of claim 1 wherein the rules include at least one of the following: subject heading rules, from heading rules, body rules and HTML rules.

7. The system of claim 5 wherein the system retires rules from the database if such rules are not matched for a predetermined period of time.

8. The system of claim 7 wherein the predetermined period of time is 30 days.

9. The system of claim 1 wherein the system is implemented on a mail server in a network.

10. The system of claim 1 wherein the system is implemented over a distributed network having a plurality of mail servers.

11. The system of claim 10 further comprising:

a program for selecting rules that have been matched within a predetermined period of time; and

wherein the system replicates the selected rules over the plurality of mail servers.

12. The system of claim 11 wherein the program stores the selected rules within files that are replicated over the plurality of mail servers.

13. The system of claim 12 wherein the files are .db files.

14. The system of claim 1 wherein the message processor attaches the data to a message by generating an encoded spam information string indicating the rules that are matched and attaching the string to the message.

15. The system of claim 14 wherein the message processor further stores encoded information strings for a plurality of messages within a log file, which is periodically communicated to the spam analyzer.

16. The system of claim 14 further comprising:

an online processing tool, which allows a user to view unfiltered spam messages submitted by clients and to decode and display the spam information strings associated with the messages.

17. The system of claim 15 wherein the online processing tool is further adapted to allow modification of the rules.

18. The system of claim 1 wherein the spam analyzer further calculates a total score for each e-mail message based on the rules matched by the message and identifies e-mail messages as spam based on their respective total score.

19. A method for analyzing and managing spam e-mail, comprising:

storing rules for determining whether e-mail messages are spam;

receiving e-mail messages;

determining whether any rules are matched by a message;

recording data regarding rules that are matched by the message;

attaching the data to the message;

analyzing the data to determine attributes regarding the rules; and

dynamically modifying the rules based on the data.

20. The method of claim 19 wherein the data is recorded in encoded spam information strings.

21. The method of claim 20 wherein the encoded spam information strings are attached to the messages as headers.

22. The method of claim 19 wherein the attributes comprise statistics.

23. The method of claim 22 wherein the statistics comprise at least one of the following: last updated, last hit, total hits, spam hits, nonspam hits, and false positive hits.

24. The method of claim 19 wherein the rules are stored within a relational database.

25. The method of claim 24 wherein the rules include at least one of the following: subject heading rules, from heading rules, body rules and HTML rules.

26. The method of claim 24 wherein each rule in the database is assigned an identification number and a score that is used to determine whether an e-mail is a spam e-mail.

27. The method of claim 26 further comprising:
calculating a total score for each e-mail message; and
identifying an e-mail message as spam based on its total score.

28. The method of claim 27 further comprising:
retiring rules from the database if such rules are not matched for a predetermined period of time.

29. The method of claim 28 wherein the predetermined period of time is 30 days.

30. The method of claim 19 wherein the e-mails are received over a distributed network having a plurality of mail servers.

31. The method of claim 30 further comprising:
selecting rules that have been matched within a predetermined period of time;
storing the selected rules within files; and
replicating the files over the plurality of mail servers.

32. The method of claim 19 further comprising:
receiving reports regarding unidentified commercial e-mail messages; and
modifying the rules based on the reports.

33. The method of claim 19 further comprising:
receiving reports regarding e-mails mistakenly identified as spam e-mail; and
modifying the rules based on the reports.